Amendments to the Specification

Please replace the paragraph at page 1, lines 7-10 with the following amended paragraph:

The present invention relates to the provision of improved security in a device which has services accessible by other devices communicating with the device. It particularly relates to devices which are accessed over a radio interface in accordance with the ~~Bluetooth~~ BLUETOOTH specification (a digital wireless protocol).

Please replace the paragraph at page 1, lines 12-26 with the following amended paragraph:

Figure 1 illustrates a network 2 of radio transceiver units, including a master unit 4 and slave units 6, 8 and 10, communicating by transmitting and receiving radio packets. There is only one master in a network. The network operates in a time division duplex fashion. The transceiver units are ~~synchronised~~ synchronized to a common time frame determined by the master unit 4. This time frame consists of a series of time slots of equal length. Each radio packet transmitted in the network has its start aligned with the start of a slot and a single packet transmitted in the network at a time. When the master unit is performing point-to-point communication a transmitted radio packet is addressed to a particular transceiver which replies to the master unit by transmitting a radio packet addressed to the master unit in the next available time slot. When the master unit is performing point to multi-point

communication a transmitted radio packet is addressed to all transceiver units. Any misalignment between the master and a slave is corrected by adjusting the timing of the slave.

Please replace the paragraph at page 1, line 28 - page 2, line 5 with the following amended paragraph:

The transceivers transmit and receive, in this example, in a microwave frequency band, illustratively 2.4 Ghz. The network reduces interference by changing the frequency at which each radio packet is transmitted. A number of separate frequency channels are assigned each with a bandwidth of 1MHz, and the frequency may hop at a rate of 1600hops/s. The frequency hopping of the transceivers communicating in or joining the network is ~~synchronised~~ synchronized and controlled by the master unit. The sequence of hopping frequencies is unique for the network and is determined by a unique identification of the master unit.

Please replace the paragraph at page 2, lines 7-10 with the following amended paragraph:

Each transceiver unit has a unique identification, the Unit ID, henceforth referred to as the ~~Bluetooth~~ BLUETOOTH ID. Each ~~Bluetooth~~ BLUETOOTH ID (48-bit IEEE address) is unique for each ~~Bluetooth~~ BLUETOOTH unit. A ~~Bluetooth~~ BLUETOOTH ID of a unit can be found through an enquiry routine over the RF interface to the unit.

Please replace the paragraph at page 2, lines 12-16 with the following amended paragraph:

The network is a radio frequency network suitable for transmitting voice information or data information between transceivers. The transmissions made are of low power, for example 0 to 20dBm, and the transceiver units can effectively communicate over the range of a few ~~centimetres~~ centimeters to a few tens or hundred of ~~metres~~meters.

Please replace the paragraph at page 3, lines 7-15 with the following amended paragraph:

Referring to Figure 4, a schematic illustration of a transceiver unit is shown. Only as many functional blocks and interconnections are shown in this diagram as are necessary to explain in the following how a transceiver unit and the communication network operates. The transceiver unit 40 contains a number of functional elements including: an antenna 46, receiver 50, ~~synchroniser~~ synchronizer 52, header decoder 54, controller 60, memory 56, ~~packetiser~~ packetizer 42, clock 68, frequency hop controller 48 and transmitter 44. Although these elements are shown as separate elements they may in fact be integrated together and may be carried out in software or in hardware.

Please replace the paragraph at page 3, lines 17-30 with the following amended paragraph:

Data to be transmitted in the payload by the transceiver unit 40 is supplied as data signal 41 to the ~~packetiser~~ packetizer 42. Control information to be transmitted in the payload of a packet is supplied in a payload control signal 87 provided by the controller 60 to the ~~packetiser~~ packetizer 42. The ~~packetiser~~ packetizer 42 also receives an access code control signal 69 and a header control signal 71 from controller 60 which respectively control the Access Code 34 and the Header 36 attached to the payload to form the packet. The ~~packetiser~~ packetizer 42 places the data or control information into a packet 30 which is supplied as signal 43 to the transmitter 44. The transmitter 44 modulates a carrier wave in dependence upon the signal 43 to produce the transmitted signal 45 supplied to the antenna 46 for transmission. The frequency of the carrier wave is controlled to be one of a sequence of hop frequencies by a transmission frequency control signal 47 supplied by the frequency hop controller 48 to the transmitter 44.

Please replace the paragraph at page 4, lines 1-24 with the following amended paragraph:

The antenna 46 receives a radio signal 51 and supplies it to the receiver 50 which demodulates the radio signal 51 under the control of a reception frequency control signal 49 supplied by the frequency controller 48 to produce a digital signal 53. The digital signal 53 is supplied to the ~~synchroniser~~ synchronizer 52 which ~~synchronises~~

synchronizes the transceiver unit 40 to the time frame of the network. The ~~synchroniser~~ synchronizer is supplied with an access code signal 81 specifying the Access Code of the packet which the transceiver unit is expecting to receive. The ~~synchroniser~~ synchronizer accepts those received radio packets with Access Codes which correspond to the expected Access Codes and rejects those received radio packets with Access Codes that do not correspond to the expected Access Code. A sliding correlation is used to identify the presence and the start of the expected Access Code. A sliding correlation is used to identify the presence and the start of the expected Access Code in a radio packet. If the radio packet is accepted then the radio packet is supplied to the header decoder 54 as a signal 55 and a confirmation signal 79 is returned to the controller 60 indicating the packet has been accepted by the ~~synchroniser~~ synchronizer 52. The confirmation signal 79 is used by the controller in a slave unit to ~~resynchronise~~ resynchronize the slave clock to the master clock. The controller compares the time at which a radio packet was received with the time at which the radio packet was expected to be received and shifts its timing to offset the difference. The header decoder 54 decodes the header in the received packet and supplies it to the controller 60 as header signal 75. The header decoder 54, when enabled by a payload acceptance signal 77 supplied by the controller 60, produces a data output signal 57 containing the remainder of the radio packet, the payload 38.

Please replace the paragraph at page 6, lines 1-5 with the following amended paragraph:

a9

The ~~Bluetooth~~ BLUETOOTH technology should provide security measures both at the application layer and the link layer. Currently, in each ~~Bluetooth~~ BLUETOOTH unit the link layer 106 security measures are ~~standardised~~standardized. Authentication and encryption routines are implemented in a standard way in each device in the Link Layer 106.

Please replace the paragraph at page 6, lines 7-11 with the following amended paragraph:

a10

Each unit stores one or more secret authentication link keys for use in communication with another unit or units. Typically a unit will permanently store a link key for each of the units it wishes to communicate with. Each link key is associated with the ~~Bluetooth~~ BLUETOOTH ID of the unit for which it is used to communicate.

Please replace the paragraph at page 6, lines 20-30 with the following amended paragraph:

a11

A challenge response scheme is used to authenticate a unit. A valid pair of units share the same secret link key. A first unit produces a random number and challenges a second unit to authenticate itself by supplying the random number to it. The second unit returns the result of a function which takes as its arguments the

~~Bluetooth~~ BLUETOOTH ID of the second unit, the received random number and the key associated with the first unit but stored in the second unit. The first unit uses the same function to produce a result which if it equals the result received from the second unit authenticates the second device. The function in the first unit takes as its arguments the ~~Bluetooth~~ BLUETOOTH ID of the second unit which has been previously obtained, the random number and the key associated with the second unit but stored in the first unit.

Please replace the paragraph at page 10, lines 1-13 with the following amended paragraph:

According to a further aspect of the present invention there is provided a device for providing services and allowing access by other devices to the provided services, comprising: an interface for communicating with the other devices and receiving requests to access a service therefrom; arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user ~~authorisation~~ authorization is required and if the requesting device has no stored trust indication associated therewith user ~~authorisation~~ authorization is requirable; and a user interface for providing user ~~authorisation~~authorization.

Please replace the paragraph at page 10, lines 15-29 with the following amended paragraph:

According to a further aspect of the present invention there is provided a device for providing services and allowing access by other devices to the provided services, comprising: an interface for communicating with the other devices and receiving requests to access a service therefrom; arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and store security indications in association with provided services and arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no user ~~authorisation~~ authorization is required and if the requesting device has no stored trust indication associated therewith user ~~authorisation~~ authorization is required in dependence upon the stored security indication associated with the requested service; and a user interface for providing user ~~authorisation~~authorization.

Please replace the paragraph at page 11, lines 1-8 with the following amended paragraph:

According to the embodiments of the invention, access to services depends upon the trust level of the device which is trying to access the service. A trusted device, once

its identity has been verified has access to all the services/applications. A not-trusted device may require user ~~authorisation~~ authorization each time it attempts to access a service. Therefore the grant of access of a not-trusted device to one service does not open up the other services to access. Separate user ~~authorisation~~ authorization is required to access each of the other services.

Please replace the paragraph at page 13, lines 1-16 with the following amended paragraph:

The lowest multiplexing protocol layer 108 sends a query to the security manager asking whether access to a higher entity such as the higher protocol layer 110 or application 18_3 should be given. This query identifies the service/application to which access is required and the ~~Bluetooth~~ BLUETOOTH ID of the device requesting access. The Security Manager determines if access to the next entity should be allowed and may control the Link Layer 106 to enforce authentication. If the querying protocol layer is not directly connected to the requested service, the Security Manager automatically sends a grant signal to the querying protocol layer 108 which then allows access to a higher protocol layer 110. If the querying protocol layer 108 is directly connected to the requested service 118_3, the Security Manager arbitrates to determine if access should be allowed. If access is allowed it sends a grant signal to the lowest multiplexing protocol layer 108 which then accesses the application 18_3. If access is denied, the Security Manager 120 sends a refusal signal

a5

to the lowest multiplexing protocol 108 preventing access of the requesting unit to the desired service.

Please replace the paragraph at page 13, line 18 - page 14, line 3 with the following amended paragraph:

The request to access a service (application 118_1 or 118_2) received at the higher multiplexing protocol 110 from the lowest multiplexing protocol 108, causes the layer 110 to send a query to the Security Manager asking whether access to a higher entity such as a higher multiplexing protocol layer (not illustrated) or application 118_1 or 118_2. This query identifies the service/application to which access is required and the ~~Bluetooth~~ BLUETOOTH ID of the device requesting access. If the querying protocol layer is not directly connected to the requested service, the Security Manager automatically sends a grant signal to the querying protocol layer 108 which then allows access to a higher protocol layer. If the querying protocol layer 110 is directly connected to the requested service, the Security Manager arbitrates to determine if access should be allowed. If access is allowed it sends a grant signal to the querying protocol layer 110 which then accesses the requested application. If access is denied, the Security Manager 120 sends a refusal signal to the querying protocol layer 110 preventing access of the requesting unit to the desired service.

a6

Please replace the paragraph at page 14, lines 22-30 with the following amended paragraph:

The Security Manager may use its interfaces to the service database 122, the device database, the link manager and the UI 130 to perform an above-mentioned arbitration. An exemplary service database is illustrated in Figure 7a and an exemplary device database is illustrated in Figure 7b. When the Security Manager receives a query from the protocol layers or applications it queries the databases 122 and 124. It accesses the fields associated with the requested application/service from the service database and accesses the fields associated with the ~~Bluetooth~~ BLUETOOTH ID of the requesting unit from the device database 124.

Please replace the paragraph at page 15, lines 1-9 with the following amended paragraph:

The databases are used to define different security levels for devices and services. Each unit has a device database which stores information about other devices it has previously communicated with. The device database has an entry for each ~~Bluetooth~~ BLUETOOTH ID of the other devices. Each entry has associated fields including a first field to indicate whether that device is trusted or not trusted, a second field for storing the current link key for communication with that devices and a third field to indicate whether there has been a successful authentication with that device in the current session.

Please replace the paragraph at page 16, lines 4-10 with the following amended paragraph:

When the security rating of the service is not-open then there is a dependence upon the trust level of the device requesting access. If the requesting device is trusted, then the device requesting access to the service must be authenticated before access to the service is granted. If the requesting device is untrusted, then the device requesting services must be authenticated and then explicit user ~~authorisation~~ authorization must be given before access to the service is granted.

Please replace the paragraph at page 17, line 25 - page 18, line 24 with the following amended paragraph:

If the requesting device is not-trusted, authentication and user ~~authorisation~~ authorization is required. If authentication of the requesting device has not occurred in this session (206) (determined from the 3rd field of the entry for the requesting device in the device database), then the security manager instructs (208) the link layer 106 to perform an authentication. The security manager provides the link layer with the current key (if any) stored in the 2nd field of the database entry. The link layer performs the authentication (with pairing if necessary) as previously described in relation to Figure 10, and informs the security manager if the authentication has been successful. If the authentication is unsuccessful the Security Manager sends (218) a refusal signal to the querying protocol thereby preventing access to the

service. If the authentication is successful the link layer also returns the current link key for the requesting device and the Security Manager updates the device database (210), placing the current link key in the second field of the database entry and indicating that successful authentication has occurred in this session in the third field of the entry. The security manager checks (212) the trusted status of the requesting device. As the device is not-trusted, the security manager then attempts to obtain user ~~authorisation~~ authorization (214) as illustrated in Figure 11. The security manager controls (230) the UI 130 to indicate to the user that some positive act is required to allow a requesting device access to a service. The service and/or the requesting device may be identified on a screen. The user can agree or disagree to the access. Agreement causes the Security Manager to give (216) a grant signal to the querying protocol layer thereby allowing access to the requested service. Disagreement causes the Security Manager to give (218) a rejection signal to the enquiring protocol thereby preventing access to the requested service. The fact that the user ~~authorisation~~ authorization has been given is not recorded and access is therefore one time only. The Security Manager, may then as an option, offer (232) the user the opportunity to change the trust status of the requesting device from untrusted to trusted with subsequent updating (234) of the device database.

Please replace the paragraph at page 19, line28 with the following amended paragraph:

6 Security Manager asks for manual user ~~authorisation~~authorization

Please replace the paragraph at page 20, lines 7-12 with the following amended paragraph:

The preceding description describes a preferred implementation of the claimed invention in a preferred application, namely a low power radio frequency communications network in accordance with the ~~Bluetooth~~ BLUETOOTH Standard. However, it should be appreciated that other implementations and applications may be ~~utilised~~ utilized without departing from the scope of the invention.

a22

Please replace the paragraph at page 20, lines 14-21 with the following amended paragraph:

In particular, in the embodiment described, whether or not the device authentication is required depends simply on the service requested and the content of the service database, in particular, whether the service is open or not-open. Whether or not user ~~authorisation~~ authorization is required is dependent on the service requested and the content of the service database, in particular, whether the service is open or not-open and dependent upon the identity of the device requesting access and the content of the device database, in particular whether the requesting device is trusted or not-trusted.

a23

Please replace the paragraph at page 20, lines 23-29 with the following amended paragraph:

It would of course be possible to make device authentication solely or additionally dependent upon the trust status of the device requesting the service. It would also be possible to make user ~~authorisation~~ authorization solely or additionally dependent upon the service requested so that, for example, user ~~authorisation~~ authorization is or is not required for a not-trusted device accessing a particular service in dependence on the stored attributes of the service.

Please replace the paragraph at page 21, lines 1-8 with the following amended paragraph:

In the above embodiments, the operation of the security architecture has been described in relation to a device requesting access to a service in the 'secure' device. The security architecture may operate in both directions so that information is not sent from the 'secure' device to another device without a decision being made by the security manager. A protocol layer, preferably the highest possible multiplexing protocol layer, and the security manager in combination arbitrate whether the information is sent or not. This arbitration may require authentication and/or ~~authorisation~~ authorization as described above.